経済産業省

資料6-1

サイバーセキュリティWGからの報告

令和元年10月4日
資源エネルギー庁
新エネルギーシステム課

サイバーセキュリティWGの概要

開催日程

第11回	2019年7月24日（水）
第12回	2019年8月29日（木）
第13回	2019年10月1日（火）

概要

- 海外のサイバーセキュリティ対策等の整理
- 実証事業者のサイバーセキュリティ対策状況整理
- 海外有識者によるガイドライン改定案のレビュー
- ガイドライン改定案の策定

出席者

【出席者】（５０音順、敬称略）

座長

梅嶋　真樹　　慶應義塾大学　SFC研究所 AUTO-IDラボ・ジャパン　副所長

学識経験者

石井　英雄　　早稲田大学　スマート社会技術融合研究機構　研究院教授
加藤　雅彦　　長崎県立大学　情報システム学部　情報セキュリティ学科　教授
小林　和真　　独立行政法人情報処理推進機構（IPA）専門委員
田居　久生　　独立行政法人情報処理推進機構（IPA）セキュリティセンター 企画部　副部長
永宮　直史　　特定非営利活動法人日本セキュリティ監査協会（JASA） 事務局長

事業者

片山　朋宏　　大阪ガス株式会社　ガス製造・発電・エンジニアリング事業部 エンジニアリング部ICTソリューションチーム
沓掛　政志　　東京電力パワーグリッド株式会社　系統運用部 系統制御グループ マネージャー
小林　将大　　エネルエックス・ジャパン株式会社　渉外部　シニアマネージャー

関係機関

青木　一彦　　電気事業連合会　情報通信部　副部長
内田　明生　　ディマンドリスポンス推進協議会　理事長
山本　敏之　　電力広域的運営推進機関　企画部　マネージャー

実証事業者

上田　智之　　関西電力株式会社 地域エネルギー本部 地域エネルギー技術グループ 部長
宇佐美　重之　　中部電力株式会社 販売カンパニー 総務部 システムグループ長
小林　輝夫　　株式会社エナリス エナリスみらい研究所 ディレクター
柴本　真吾　　東京電力ホールディングス株式会社 経営技術戦略研究所 リソースアグリゲーション推進室 課長
浜口　智洋　　東北電力株式会社 企画部 デジタルイノベーション推進室 課長
樋口　智治　　株式会社ローソン 開発本部 建設部 シニアマネジャー
福本　淳二　　アズビル株式会社　ビルシステムカンパニー マーケティング本部 環境マーケティング部環境制御グループ　マネージャー
宮原　泰徳　　KDDI 株式会社 ライフデザイン事業本部 エネルギービジネス本部 エネルギービジネス企画部 担当部長
見山　雅英　　九州電力株式会社 テクニカルソリューション統括本部 総合研究所 系統高度化グループ長
矢野　雄一　　SB エナジー株式会社 戦略事業本部 IoT 事業部 マネージャー
淀瀬　健司　　豊田通商株式会社 再生・新規電力事業部 新規事業グループ 課長補

【経済産業省】

省エネルギー・新エネルギー部　新エネルギーシステム課
電力・ガス事業部　電力基盤整備課
商務情報政策局　情報産業課
商務情報政策局　サイバーセキュリティ課

今年度のサイバーセキュリティＷＧの検討項目

- 今年度のサイバーセキュリティWGにおいては、以下の(1)～(3)の検討を進める予定。

（１）海外事業者のサイバーセキュリティ対策状況の調査

- 欧米におけるサイバーセキュリティ規制の動向整理

（２）ERABサイバーセキュリティガイドライン改定案のレビュー、改定案策定

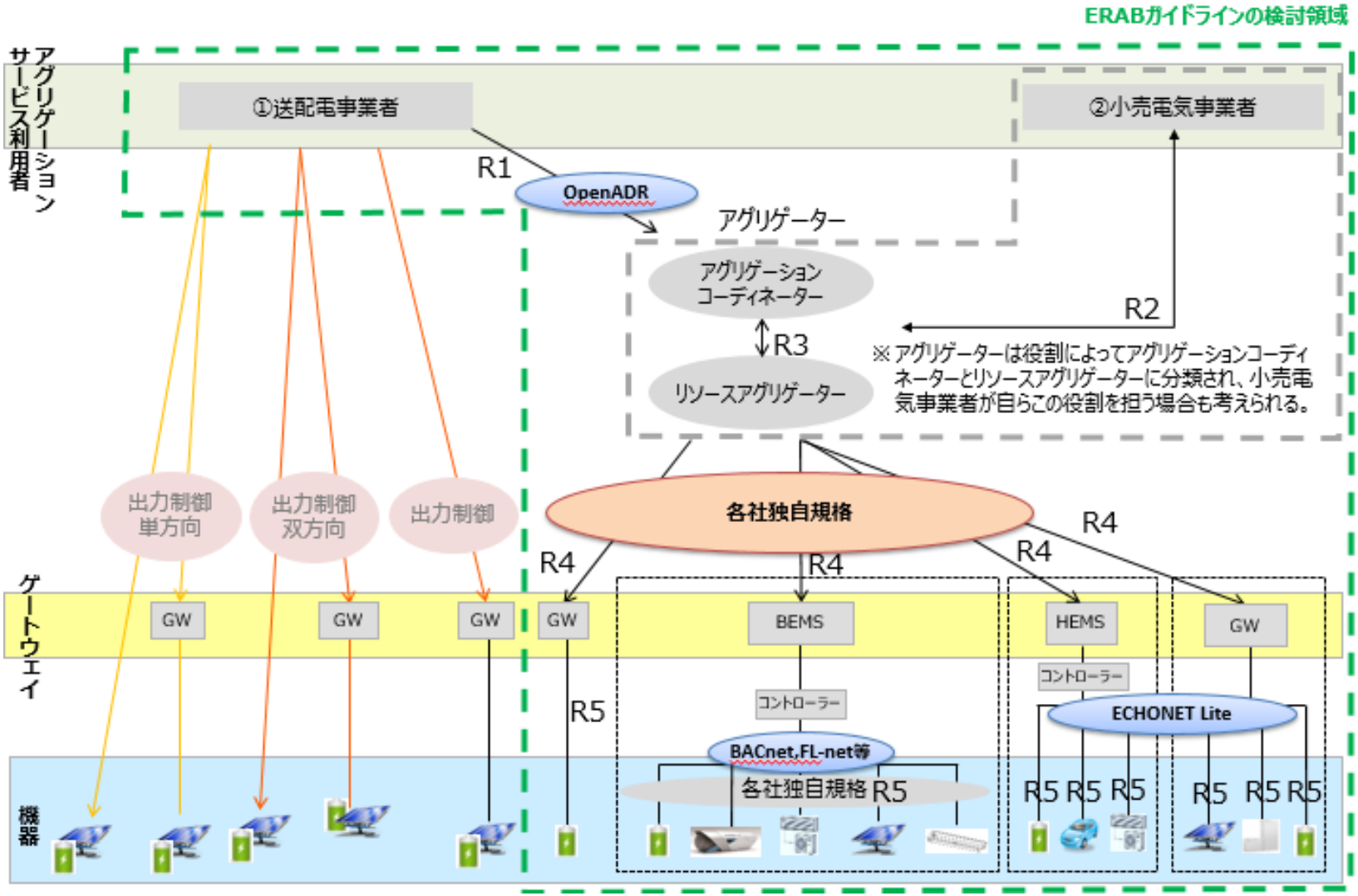
- サイバーセキュリティに関する海外有識者を招聘し、ERABシステムのサイバーセキュリティガイドラインのレビューを実施
- 有識者レビュー結果を踏まえ、ガイドライン改定版（1.3版）を策定

（３）ERABサイバーセキュリティガイドライン改定版の策定

- 2019年度下期に実施予定のパブコメ結果を踏まえ、ガイドライン改定版を確定

ERABサイバーセキュリティの概念図

- リソースアグリゲーターの制御指令を、①BEMS/HEMSが受信するケース、②ゲートウェイ（GW）が受信するケースを区別するため、記載内容の見直しを実施した。



ERABサイバーセキュリティガイドライン

- ERABサイバーセキュリティガイドラインは、アグリゲーターをはじめとする**ERAB事業者が取り組むべきサイバーセキュリティ対策**を整理したもの。

ERABセキュリティガイドラインの概要

1. ガイドラインの位置づけ
- 「電力制御システムセキュリティガイドライン」と「IoT開発におけるセキュリティ設計の手引き」の考え方に基づき、事業者が実施すべき最低限のセキュリティ対策を整理したもの。
- 事業者が実装を必須として義務付けられる【勧告】、と実装を検討すべき【推奨】に分けて規定。

2. ERABシステム
- システム構成
- 基本方針
- 想定すべき脅威
- 維持すべきサービスレベル
- システム重要度の分類
- サイバーセキュリティ対策
- 取り扱い情報の差異によるシステムの分類
- 詳細対策要件の設計
- ガイドラインの継続的改善

3. 事業者における対策の在り方
- 本ガイドラインを標準対策要件とし、事業者が実運用に耐えうる「詳細対策要件」を策定

【参考】海外有識者によるERABサイバーセキュリティガイドラインのレビュー

- フランスより電力分野のサイバーセキュリティ対策について知見のある有識者を招聘し、有識者を含めたWGの開催及び有識者によるガイドラインのレビューを実施した。

第12回サイバーセキュリティWG

日時：2019年8月29日（木）13:00~15:00
場所：慶應義塾大学三田キャンパス
参加者：海外有識者3名＋サイバーセキュリティWGメンバー

海外有識者のプロフィール

① **Kave Salamatian**氏
The Computer Science, Systems, Information and Knowledge Processing Laboratory (LISTIC) 教授 ※日仏サイバーセキュリティ会議メンバー

② **Claude Kirchner**氏
President of IRB, INRIA（フランス国立情報学自動制御研究所）※日仏サイバーセキュリティ会議メンバー

③ **Richard Schomberg**氏
IEC ambassador, VP, Smart Grid Standard, EDF

【参考】海外調査結果

- 欧米においても電力システムを対象とした規制やガイドラインが存在するが、ERABセキュリティガイドラインで示されたセキュリティ対策要件と大きな乖離は見られない。

日米欧における電力分野のサイバーセキュリティ対策基準の比較

- 欧米諸国では、重要電力設備（系統制御、大規模発電設備等）に対して、サイバーセキュリティに関する公的な規制が存在する。
- 一方、分散型電源に関するシステム（スマート電力システム）に対しては、自主的対策を基本としたガイドライン等が示されている。

日米欧における電力分野のサイバーセキュリティ対策基準の整備状況

対象	日本	米国	欧州 ・ 国際標準
重要電力設備 系統信頼性制御、大規模需給調整制御、大規模な発送電等を行うシステム	公的規制 / 強制 （電気事業法技術基準の解釈による） **電力制御システムセキュリティガイドライン** （組織・システムの対策）	公的規制 / 強制 （連邦電力法による） **NERC Critical Infrastructure Protection (CIP) Standard** （組織・システムの対策）	公的規制 / 強制 （NIS指令） **EU各国が対策基準を明確化することを指示** （組織の対策） 国際標準 / 任意／第三者認証 **ISO/IEC 27019*** Information security controls for the energy utility industry （組織・システムの対策）
スマート電力システム アグリゲーター、分散電源管理、需要家電源管理、等を行うシステム	（実証ガイドライン） **ERABに関するサイバーセキュリティガイドライン** （組織・システムの対策）	ガイドライン / 任意 **NISTIR 7628** Guidelines for Smart Grid Cyber Security （組織・システムの対策）	国際標準 / 任意 **IEC 62351*** Power systems management and associated information exchange - Data and communications security - （システムの対策）

*ISO/IEC 27019 および IEC 62351 は重要電力設備、スマート電力システム双方を対象とする

出所）各種ガイドライン・国際規格より三菱総研作成

（出所）第11回サイバーセキュリティWG 三菱総合研究所提出資料

サイバーセキュリティWG委員及び海外有識者からの主な意見１/２

- WGや海外有識者によるレビュー等において、ERABサイバーセキュリティガイドラインに対して、主に以下の観点について意見が出された。

① サイバー・フィジカルの相互運用性の確保

- ERABシステムは単に情報システムであるだけでなく、電力も制御するサイバー・フィジカル・システムであり、国民や産業にも影響があるという認識の下、検討する必要がある。

② 国際標準の参照

- 国際標準はERAB事業者のセキュリティ対策をサポートするものとして、その取扱を検討すべきである。

③ 事故発生時の対応

- サイバー攻撃が発生した場合には誰の責任なのか明確にできるようデータ管理する必要がある。
- 現行のガイドラインは、事故発生時の対処に関する記載が不足している。
- 関係機関への報告や復旧対応のあり方を検討することも有効である。
- インシデント検知のためにログを取得することを明記したほうがよい。

④ 事業者の責任範囲

- アグリゲーションコーディネーターの責任範囲を議論すべきである。

サイバーセキュリティWG委員及び海外有識者からの主な意見２/２

⑤ 第三者認証

- 監査コストが参入障壁にならないよう配慮しつつ、第三者監査に関する監査人の力量や公平性といった要求を定義する必要はある。
- 一定の基準を満たした上での自己監査を許容する等の柔軟性も議論すべき視点である。

⑥ 勧告項目の実装の実現性の検証

- 要求事項を課した場合はその要求が守られていることを確認する必要がある。

⑦ ERABに求められる要求事項の明確化

- システムの要件は、透明性が担保されているか等、詳細な設計を行う必要がある。

⑧ ERABに求められるセキュリティ水準に関する認識の共有

- 各事業者において作成する詳細対策要件のレベル感にバラつきが生じないようにすべきである。
- 用語の意味や範囲に対する理解が人によって異なるため、範囲を必要以上に狭めないよう留意しつつ明確にしたほうが良い。
- セキュリティに関する情報を共有できる仕組みが必要ではないか。
- 一定の水準を担保するために、ガイドラインと詳細対策要件の間をつなぐ解釈集のようなものが必要ではないか。

改定案（Ver1.3）のポイント（１/４）

- WGの委員や有識者からの意見に対して対応方針を検討し、ERABサイバーセキュリティガイドラインの改定案として反映した。主な反映事項を下記のとおり示す。

①サイバー・フィジカルの相互運用性の確保

意見
- ERABシステムは単に情報システムであるだけでなく、電力も制御するサイバー・フィジカル・システムであり、国民や産業にも影響があるという認識のもと検討する必要がある。

対応案
- 【pp.4-5】ERABシステムはサイバー・フィジカル・システムであり、一般的なITシステムとは異なり情報の保護だけでなく、物理システムに対するレジリエンスを確保する必要があることを追記。併せて、経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」を引用。

②国際標準の参照

意見
- 国際標準はERAB事業者のセキュリティ対策をサポートするものとして、その取扱を検討すべきである。

対応案
- 【p.17 第4.1.3項】ERAB事業者が、PDCAサイクルに則ったセキュリティ対策の実施や改善をする際に国際標準が役立つことを追記。

※【 】内は意見を踏まえて加筆修正したガイドラインの箇所を示す。

改定案（Ver1.3）のポイント（２/４）

③事故発生時の対応

意見

- サイバー攻撃が発生した場合には誰の責任なのか明確にできるようデータ管理する必要がある。
- 現行のガイドラインは、事故発生時の対処に関する記載が不足している。
- 関係機関への報告や復旧対応のあり方を検討することも有効である。
- インシデント検知のためにログを取得することを明記したほうがよい。

対応案

- 【p.8 第3.3節】インシデント対策として、システムのログを取得することを記載。
- 【p.10 第3.6節】Step７として、事故発生時の対応方法の設計・運用・訓練について記載。
- 【p.18 第4.1.4項】ERAB事業者は、インシデント発生時の被害を考慮し、被害を最小限にとどめるための対応及び対応体制を構築することを記載。

④事業者の責任範囲

意見

- アグリゲーションコーディネーターの責任範囲を議論すべき。

対応案

- 【p.10 第3.6節】Step１として、システムの全体構成及び責任分界点を明確化するよう記載。

※【 】内は意見を踏まえて加筆修正したガイドラインの箇所を示す。

改定案（Ver1.3）のポイント（３/４）

⑤第三者認証

意見
- 監査コストが参入障壁にならないよう配慮しつつ、第三者監査に関する監査人の力量や公平性といった要求を定義する必要はある。
- 一定の基準を満たした上での自己監査を許容する等の柔軟性も議論すべき視点である。

対応案
- 【p.10 第3.6節】Step６として、第三者による監査（認証を含む）や教育プログラム等による勧告項目の実装を検証と記載。

⑥勧告項目の実装の実現性の検証

意見
- 要求事項を課した場合はその要求が守られていることを確認する必要がある。

対応案
- 【p.10 第3.6節】Step６として、第三者による監査（認証を含む）や教育プログラム等による勧告項目の実装を検証と記載。
- 【p.16 第4.1節】勧告事項として、ERAB事業者に対するセキュリティ教育及び訓練の実施とその効果の確認について記載。

※【 】内は意見を踏まえて加筆修正したガイドラインの箇所を示す。

改定案（Ver1.3）のポイント（４/４）

⑦ERABに求められる要求事項の明確化

意見

- システムの要件は、透明性が担保されているか等、詳細な設計を行う必要がある。

対応案

- 【p.8 第3.2節】ERAB参画事業者に対して、脆弱性対策情報・脅威情報の共有の取組について定め、それについて協力することを勧告項目として記載。具体は、各事業者の詳細対策要件で定める。
- 【p.10 第3.6節】Step１として、システムの全体構成及び責任分界点を明確化するよう記載（再掲）。
- 【p.11 第3.6.1項】誰に対する責任か明確にするため、送配電事業者に対して責任を持つと記載。
- 【p.16 第4.1節】セキュリティ管理責任者の任命に加え、管理者間での共有体制構築を記載。

⑧ ERABに求められるセキュリティ水準に関する認識の共有

意見

- 各事業者において作成する詳細対策要件のレベル感にバラつきが生じないようにすべきである。

対応案

- ガイドラインとは別に、一定のセキュリティ水準を満たす詳細対策要件を策定する上で参考となる「ERABサイバーセキュリティガイドライン解釈集（仮）」を作成する。

※【 】内は意見を踏まえて加筆修正したガイドラインの箇所を示す。

今後の進め方

- 関連する審議会・検討会等の議論と整合性を保つことを確認した上で、パブリックコメントで広く意見を聴取しガイドラインを改定する。
- また、ガイドラインの改定と併せて、一定のセキュリティ水準を満たす詳細対策要件を策定する上で参考となる「ERABサイバーセキュリティガイドライン解釈集」を策定する。